Procedures to Comply with HSC Mobile Device Security Standard

Personal mobile devices that are used to access the UNM HSC network must conform to the security requirements outlined in the HSC's Information Technology Standards for Users

- Reference: http://hsc.unm.edu/library/usersupport/IT_Standards.shtml para 5.0

Recovery software. All portable computers (laptops and tablets) owned by the University or the HSC Research Institutes must have tracking data or software installed to enable their identification and retrieval in the event of loss or theft.

- Modify the Bios or hard drive to identify the University as the owner.

- Install a form of lojack device to track the computer once it is turned on, ie Computrace.

Physical protection. Mobile devices owned or issued by the University must not be left unattended in a public space and, where possible, must be physically locked away or secured.

- Mobile devices can be secured in a single occupancy office where a door can be locked.

- If the door does not have a locking device, the the mobile device must be secured in a cabinet or drawer that does lock.

- In a large office area comprised of cubicles with no locking doors or open tops that can be climbed over, then the mobile device should be secured in a locking drawer or cabinet.

- Use of mobile devices in public areas such as an internet cafe, lobby or outside, etc, must not be left unattended for any reason, ie, trip to bathroom or refill of coffee, etc.

- Mobile devices should not be left in open view of a parked vehicle. If stops are required while in transit, mobile devices will be stored in the trunk of a vehicle, behind the seat of a pickup, or if in an SUV, should be covered to conceal it. If these precautions can not be taken, then the stop is not recommended.

- Mobile devices will not be left in any vehicle, overnight.

- Mobile devices will not be "loaned" out to friends or acquaintances.

Device identification. All laptops, tablets, PDAs, Blackberries, smart phones and portable hard drives owned or issued by the University must be permanently marked as "Property of the University of New Mexico or UNM Hospitals" and indicate a method of return if the device is lost.

- Although the University tags equipment with a UNM tag sticker, these can be removed. Possible solutions could be a black light pen. Marking the device so when scanned with a black light will reveal the asset as a University mobile device.

- Etching with an engraver.

- Coordinate with Dell to have the official UNM logo permanently branded on the body of the laptop. This does not cover other mobile devices, however.

- A simple sticker, of various sizes, to affix to the mobile device identifying it as a University asset and directions for returning the device.

- Use of a Sharpie.

Virus protection. Any HSC mobile device that is capable of using antivirus software must have the software installed and configured to maintain updated virus software and signatures. Contact Information Security (2-DATA,2-1694) for information on approved antivirus software.

- For laptops, contact the HSLIC Helpdesk at 272-1694 to install this feature.

- For personal devices, contact the HSC IT Security Officer for information on approved antivirus software.

- All others, please contact your service provider, ie blackberry, iphone, etc.

Security Updates. A procedure must be established and implemented to ensure that all security patches and updates relevant to the device or installed applications are promptly applied in compliance with the HSC's Standards.

- Cell phones should be powered off at least once a week so that it may reboot and receive updates from your carrier/provider/vendor.

- For laptops, call the HSLIC Help Desk at 272-1694 for assistance.

- All others, contact your service provider.

Disable unused services. Wireless, infrared, Bluetooth or other connection features should be turned off when not in use.

- Open connections can be vulnerable. Turn off devices when not in use and do not leave open connections.

Storage of passwords. The storage of user IDs and passwords which allow access to the HSC network or its systems is prohibited on all mobile devices, unless done in accordance with approved HSC Standards.

- ID's and passwords stored on mobile devices is discouraged, however, may be permitted if stored in an encrypted state and utilize secure transmission, SSL.

Termination of University relationship. All University-owned mobile devices must be returned to the appropriate HSC department immediately upon termination of the assigned user's relationship with the department or University. In addition, any software applications purchased by the University and installed on personal mobile devices must be removed immediately by the user.

- From the control panel, select Add/Remove software. Select all University provided software.

- Return all mobile devices owned by the University to your immediate supervisor. Ensure your termination checklist is marked appropriately.

- The supervisor will receive the mobile devices and make the proper reporting to the equipment custodian of the new owner/location of the mobile devices, or proper documentation of the surplusing.

Report any suspected misuse or theft of a mobile device immediately to Information Security and the campus police.

- Call the HSC IT Information Security Officer, Barney Metzner at 272-1696.

- Call the UNM Campus police at 277-2241.

- Call the HSC Hotline at 1-888-899-6092.

Reference:

5.0 Security Standards

5.1 Security/Passwords

Each employee is individually responsible for maintaining their passwords, including changing the=m regularly (180 days or sooner), in accordance with the UNM Account Password Standard(http://cio.unm.edu/standards/) and HIPAA mandated HSC password protection policy and procedures. (http://hospitals.unm.edu/policiies_and_procedures/index.cfm). Doing so will help assure the security and integrity of individually identifiable and business critical information. Users of UNMH IT managed systems are required to attend training and sign a confidentiality statement before receiving system access.

5.2 Virus Scanning and Data Backup

All UNM or UNMH desktops and servers connected to campus networks must have current virus scanning installed and actively scanning the appropriate file systems. McAfee VirusScan is the current, centrally managed and site-licensed virus protection software available at no cost for all HSC computers running Windows XP Professional or Vista. It is therefore strongly recommended that HSC and UNMH users use McAfee's VirusScan unless there is a significant business need to install a different product.

All connections on the network are continuously monitored for malicious activity that is the result of a virus infection or system compromise. Given the criticality of the HSC network, the network connection/port of an infected/compromised machine will be disabled until the issue is addressed and approved for reactivation by one of the HSC Help Desks.

All centralized systems supported by UNMH IT and HSLIC are backed up in accordance with best practices and HIPAA legislation. Individual users in cooperation with systems administrators should develop a regular system and data backup procedure for workstations and departmental servers. Everyone should recognize that they are responsible for data stored on local system drives. Those who maintain mission critical servers and services should use current enterprise class business continuity procedures including: off-site storage, automated media rotation and redundancy. All backup and business continuity procedures should be reviewed annually in reference to the HSC IT Disaster and Contingency Plan Policy which can be found at: http://hospitals.unm.edu/policies_and_procedures/index.cfm.

5.3 Employee Data Backup

The HSC provides network storage for employees, H: drive for UNMH users, and H: and O: drives for all other HSC users. Network storage is easily accessible, privileged and shared. It is also regularly backed up. Network storage includes shared file space for individual departments / units and “Home” directories for individual users. Employees are encouraged to store work product in the appropriate location.

UNM’s Acceptable Computer Use Policy (University Business Policies and Procedures Manual, policy 2500) allows for the incidental personal use of personal files. In order to control costs incidental use is limited to storage on local drives. Certain file type kept on shared network storage will be subject to additional restriction and quotas; (temporary files, ~*.tmp; binary executables, *.exe, *.dll, etc.)

Backups by central IT are limited to official shared network storage; local files are not backed up by central IT, check with local departmental support for more info. Files can only be restored for file saved on official shared network storage. Files stored on network drives for at least 48 hours can be restored for up to 2 weeks. Files existing on network storage for longer than 30 days can be restored for up to a one year. The version of the file restored is based on the time it was backed up and after 2 weeks only one version per month is available. Restoration of file older than one year is rarely feasible due to resources and technology limits. Special arrangements should be made for long term archiving or other file storage needs requiring additional resources for backup, large storage quotas, high performance access, etc. Please contact the help desk to make arrangements. For the most recent standards and examples of appropriate use of network storage please see: http://hsc.unm.edu/library/usersupport/wbackup.shtml.